AMENDMENTS

IN THE CLAIMS:

Please amend claims 1, 14 and 20-21 as provided below:

1. (Currently amended): A high speed add rotate add system, comprising:

a first rotator operable to receive a first input and a shift control signal for rotating the first input;

a carry save adder operable to receive a second input, a third input and the rotated first input, the carry save adder operable to sum the second input, third input and rotated first input, and to output a sum and carry output;

a shift decoder operable to receive and decode the shift control signal and output a carry control signal decoded therefrom; ~~and~~

a carry select propagating adder operable to receive the sum and carry outputs from the carry save adder and the carry control signal from the shift decoder, the carry select propagating adder operable to manipulate data contained within the sum and carry outputs based upon the carry control signal from the shift decoder and to output a result coincident with a summation of the first, second and third inputs; and

a second rotator operable to receive the result of the carry select propagating adder and the shift control signal, and rotate the result of the carry select propagating adder based thereon, and output the rotated result.

2. (Original): The system of claim 1, the first, second and third inputs have a bit length of X, where X is a positive integer.

3. (Original): The system of claim 2, wherein the carry save adder comprises a plurality of full adders, wherein respective full adders are operable to sum corresponding bits of the second input, third input and rotated first input.

4. (Original): The system of claim 3, wherein the carry save adder comprises X number of full adders.

5. (Original): The system of claim 2, wherein the carry select propagating adder comprises a plurality of full adders.

6. (Original): The system of claim 5, wherein the carry select propagating adder comprises X number of full adders.

7. (Original): The system of claim 1, wherein the carry select propagating adder comprises carry generation logic that is operable to receive the carry control signal from the shift decoder and to adjust the output of the carry select propagating adder based upon the carry control signal.

8. (Original): The system of claim 7, wherein a bit of the output of the carry select propagating adder is assigned a zero if a corresponding bit of the carry control signal is zero.

9. (Original): The system of claim 1, wherein the shift control signal is based upon $\log_2 X$, where X is a positive integer.

10. (Original): The system of claim 9, wherein the shift decoder operates according to

```
for (i=1; i<X; i=i+1)
carry control signal[i] = ~ (i == shift control signal).
```

11. (Original): The system of claim 1, wherein a path from the first input to the first rotator to the carry save adder to the carry select propagating adder and out through the second rotator is a critical path.

12. (Original): The system of claim 1, wherein the sum output corresponds to an exclusive OR operation performed on three one bit inputs.

13. (Original): The system of claim 1, wherein the carry output corresponds to an OR operation performed on respective results from three AND operations performed on three possible two input combinations for three one bit inputs.

14. (Currently amended): The system of claim 1, wherein the carry save adder performs according to the following truth table:

first input	second input	third input	carry	Sum
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

.

15. (Original): The system of claim 1, wherein the add rotate add operation is implemented in performing an HMAC-MD5-96 algorithm.

16. (Original): The system of claim 1, wherein the add rotate add operation is implemented in an IPsec module.

17. (Original): The system of claim 1, wherein the add rotate add operation is implemented in an RX IPsec processor.

18. (Original): The system of claim 1, wherein the add rotate add operation is implemented in an TX IPsec processor.

19. (Original): The system of claim 7, wherein a bit of the carry output is assigned a zero if a corresponding bit of the carry control signal is zero.

20. (Currently amended): The system of claim 1, wherein the carry select propagating adder operates according to:

P[i] = A[i] XOR B[i]
G[i] = A[i] AND B[i]
S[i] = P[i] XOR C[i]
C[i+1] = G[i] OR C[i] AND P[i]

and

C[0] = C[4]'
C[1] = CS[1] AND C[1]'
C[2] = CS[2] AND C[2]'
C[3] = CS[3] AND C[3]'

and

C[1]' = G[0] OR P[0] AND C[4]'
C[2]' = G[1] OR P[1] AND C[1]' = G[1]+P[1]G[0]+P[1]P[0]C[0]'
C[3]' = G[2] OR P[2] AND C[2]' =
G[2]+P[2]G[1]+P[2]P[1]G[0]+P[2]P[1]P[0]C[0]'
C[4]' = G[3] OR P[3] AND C[3]' =
G[3]+P[3]G[2]+P[3]P[2]G[1]+P[3]P[2]P[1]G[0]+P[3]P[2]P[1]P[0]C[0]'.

21. (Currently amended): A method of performing a fast add rotate add operation using an add rotate adder having a first rotator, a shift decoder, a carry save adder, a carry select propagating adder, and a second rotator, the method comprising:

performing a rotation operation on a first input using the first rotator according to a shift control signal;

adding the rotated first input, a second input and a third input using the carry save adder and the carry select propagating adder to obtain a sum and a carry;

decoding a carry control signal from the shift control signal using the shift decoder~~; and~~

~~adjusting~~ manipulating data contained within the sum and carry using the carry select propagating adder, based upon the carry control signal from the shift decoder and outputting a result coincident with the summation of the rotated first, second and third inputs; and

performing a rotation operation on the output result of the carry select propagating adder according to the shift control signal and outputting the rotated result thereof.

22. (Original): The method of claim 21, wherein at least one of: the first, second and third inputs have a bit length of X and the shift control signal is based upon $\log_2 X$, where X is a positive integer.